33

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-289327
(43)Date of publication of application : 19.10.1999

(51)Int.Cl. H04L 9/32
G06F 13/00
H04L 9/08

(21)Application number : 10-089097
(22)Date of filing : 01.04.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NISHIMURA TAKUYA
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI

(54) DATA TRANSMITTER, DATA RECEIVER AND MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve reliability on secrecy protection of a control key, without increasing actual loads.
SOLUTION: An STB 100 is equipped with an enciphering means 101 to allow a work key Kw to encipher AV data, a transmission side recognition means 102, which performs recognition with a VTR 200 and enciphers the Kc, a Kc generation function selection means 103 which incorporates plural functions and their function identifiers in advance and selects any one of the functions, a random numbers generation means 104 to generate random numbers Kc' to be used in generating the Kc, a Kc storage means 105 for storing the already generated Kc, a Kc generation means 106 for generating a new Kc by using part of the Kc generated in the past, the outputted random numbers Kc' and a selected function fi with these as variable, and a Kw enciphering means 107 for enciphering the Kw by using the generated Kc.

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

CLAIMS

[Claim(s)]

[Claim 1] A transfer-request reception means to receive the data transfer demand from a data sink, A data transfer means to perform a data transfer to said data sink based on said transfer request, A 1st encryption means to encipher said data transmitted based on the predetermined work-piece key Kw, A 2nd encryption means to encipher based on a control key Kc and to send the work-piece key Kw to said data sink, A secrecy element generating means to generate the secrecy element used for generation of said control key Kc, All or a part of control keys Kc generated in the past, and said generated secrecy element, It has a control-key generation means to generate the new control key Kc, using the 1st function which makes them a variable. The data source characterized by being what transmits said secrecy element to said data sink which has said 1st function when said control key Kc is newly updated.

[Claim 2] A transfer-request reception means to receive the data transfer demand from a data sink, A data transfer means to perform a data transfer to said data sink based on said transfer request, A 1st encryption means to encipher said data transmitted based on the predetermined work-piece key Kw, A 2nd encryption means to encipher based on a control key Kc and to send the work-piece key Kw to said data sink, A control-key generation means to generate the new control key Kc, All or a part of control keys Kc generated in the past, and said newly generated control key Kc, It has a secrecy element generation means to generate a secrecy element, using the 2nd function which makes them a variable. The data source characterized by

being what transmits said secrecy element to said data sink which has the inverse function of said 2nd function when said control key Kc is newly updated.
[Claim 3] While decoding a transfer-request means to give a data transfer demand to the data source according to claim 1 or 2, and the enciphered work-piece key Kw which is transmitted from said data source based on said transfer request by the control key Kc A decryption means to decode the enciphered data based on the work-piece key Kw, A hysteresis information storage means to memorize said control key Kc already used for decode of said work-piece key Kw as hysteresis information, A function storing means to store said the 1st function or said inverse function, and said the 1st function or inverse function stored, All or part of past control keys Kc memorized by said hysteresis information storage means The data sink characterized by having a control-key generation means to generate the new control key Kc, based on said secrecy element transmitted from said data source according to claim 1 or 2.
[Claim 4] The control key Kc of said past used by the initial stage by said control-key generation means when requiring a data transfer from from while having already performed said data transfer with data sink with said another data source is a data sink according to claim 3 characterized by being said not control key Kc memorized by said hysteresis information storage means but the control key Kc transmitted from said data source.
[Claim 5] The data source according to claim 1 or 2 characterized by transmitting to said data sink by making into initial information coding information in which the variable of said 1st function which said data sink has, or said inverse function contains said control key Kc in the stage when generating a control key Kc runs short of when the purport which performs said transfer is determined.
[Claim 6] The data source according to claim 1 or 2 characterized by transmitting to said data sink by making said variable with which the variable of said 1st function which said data sink has, or said inverse function contains said secrecy element in the stage when generating a control key Kc runs short of, and which run short into initial information when the purport which performs said transfer is determined.
[Claim 7] When the purport which performs said transfer is determined, the variable of said 1st function which said data sink has, or said inverse function In the inside of the stage when generating a control key Kc runs short of, and the first half of (1) The data source according to claim 1 or 2 characterized by transmitting to said data sink in the second half of the first stage by making said variable which contains said secrecy element in the second half of (2) in the first half of the first stage by making coding information containing said control key Kc into information and, which run short into information.
[Claim 8] The data sink according to claim 3 with which said initial information transmitted from the data source according to claim 5 is decoded in the stage which wants the variable of said 1st function or said inverse function for generating a control key Kc, it has an extract means to extract said control key Kc, and said

decryption means is characterized by using said extracted control key Kc for said decode.
[Claim 9] The data sink according to claim 3 characterized by said control-key generation means generating said control key Kc using said initial information transmitted from the data source of said six publications, and said function in the stage which wants the variable of said 1st function or said inverse function for generating a control key Kc.
[Claim 10] In said first half the inside of the stage which wants the variable of said 1st function or said inverse function for generating a control key Kc, and (1) -- In said second half information is decoded in said first half of the first stage in which it is transmitted from the data source according to claim 6, and said control key Kc extracts -- having -- (2) -- [moreover,] The data sink according to claim 3 characterized by generating said control key Kc in said second half of the first stage in which it is transmitted from the data source according to claim 6 using information and said function.
[Claim 11] The medium characterized by recording the program for making a computer perform any of claims 1-10, or all or a part of means of each means of one publication.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the data source, a data sink, and a medium.
[0002]
[Description of the Prior Art] A satellite broadcasting service receiver (this only being hereafter called STB) receiving, and recording on videotape the TV program sent by satellite broadcasting service with the VTR equipment connected to the receiver, or viewing and listening to it on television conventionally, is performed.
[0003] in this case, conditional [that by which record is forbidden in the image and voice data broadcast and conditional / record of is enabled only once] -- there are data. Therefore, in order to keep these conditions, it will be the requisite that recognize this condition correctly and a user side uses the equipment which operates to normal.
[0004] Then, when transmitting data recordable once from STB, for example to VTR equipment, usually authentication and key exchange (AKE) actuation for checking first whether the VTR equipment is the above regular VTR equipments are performed.

[0005] And when this authentication is not materialized, the VTR equipment used as the object for authentication is recognized as it being inaccurate equipment, and it is made not to transmit data to such inaccurate equipment.
[0006] Hereafter, it explains focusing on the conventional the configuration and authentication actuation of STB and each terminal unit, referring to drawing 6 .
[0007] Drawing 6 is the block diagram showing the conventional connection situation and conventional configuration of STB and each terminal unit, such as VTR equipment.
[0008] As shown in this drawing, an antenna 1010 is a means to receive the broadcasting electric-wave from a satellite, and STB1020 is a means to change the broadcasting electric-wave which received into AV data. The data transmission line 1070 is a bus line for the data transmission in which STB1020 and each terminal unit described below were formed in between. moreover -- a terminal unit -- ****** -- VTR -- equipment -- (-- A --) -- 1030 -- VTR -- equipment -- (-- B --) -- 1040 -- a recording apparatus -- (-- C --) -- 1050 -- TV equipment (D) is further connected with STB1020 by the data transmission line 1070.
[0009] Next, the internal configuration of STB1020 is described further, referring to this drawing.
[0010] That is, the receiving means 1021 is a means to link directly with an antenna 1010, to restore to the received data, to cancel the scramble for broadcast given to the received data, and to separate the received data multiplexed further. The encryption means 1022 is a means to encipher AV data outputted from the receiving means 1021 by the work-piece key Kw for the encryption which it had beforehand with a compression condition. Moreover, the control key Kc is beforehand built in STB1020, and is a key for enciphering the work-piece key Kw with an encryption means. Furthermore, the encryption means 1022 is a means to encipher a control key Kc with the authentication means 1023 using the subkey generated as a result of the authentication actuation mentioned later again.
[0011] The authentication means 1023 is a means to perform authentication using a predetermined secrecy function and to generate the subkey Ksa corresponding to an authentication partner as the result in order to confirm mutually whether each other's both equipments are equipment of normal between the terminal units which have carried out AV data transfer demand. Moreover, the authentication means 1023 makes all the secrecy functions (Sa, Sb, Sc, Sd, .., Sn, ...) of the proper which all terminal units have correspond with those identification numbers, and is held. The data transfer means 1024 is IEEE1394 known as a digital interface. The data transfer means 1024 is a means to perform two transfers, the isochronous transfer suitable for a data transfer like the image for which the guarantee of real time nature is needed, or voice, and the asynchronous transfer suitable for a transfer of a data for authentication, a command, etc. without the need. In addition, AV data by which encryption was carried out [above-mentioned] are sent to the data transfer means 1024 from the encryption means 1022. Moreover, the work-piece key by which

encryption was carried out [above-mentioned], and the enciphered control key are sent to the data transfer means 1024 from the authentication means 1023.
[0012] In addition, the enciphered AV data Kw (AV), the enciphered work-piece key Kc (Kw), and the enciphered control key Ksa (Kc) are sent to the terminal unit of VTR equipment 1030 grade from the data transfer means 1024.
[0013] Next, the internal configuration of VTR equipment (A) 1030 is described further.
[0014] The data transfer means 1031 is the same means as the data transfer means 1024, and is a means to receive the enciphered work-piece key and enciphered AV data as shown in this drawing. The authentication means 1032 is a means to have the secrecy function Sa of a proper beforehand, to generate the subkey Ksa as a result of authentication, and to output to the decryption means 1033. The decryption means 1033 is a means to decode the enciphered control key Ksa (Kc) which was obtained from the data transfer means 1031 by the subkey Ksa, to decode the work-piece key Kc (Kw) enciphered by this decrypted control key Kc, and to decode the AV data Kw (AV) enciphered by that decrypted work-piece key Kw. Record / playback means 1034 is a means to record decrypted AV data and to reproduce the record data.
[0015] in addition -- others -- a terminal unit -- it is -- VTR -- equipment -- (-- B --) -- 1040 -- a recording device -- (-- D --) -- 1050 -- TV -- equipment -- (-- D --) -- 1060 -- record / playback means -- removing -- the configuration and basic target of the above-mentioned VTR equipment (A) 1030 -- being the same . However, the secrecy functions which each authentication means has beforehand will be Sb, Sc, and Sd, if it says in order of each above-mentioned equipment. Therefore, the subkeys generated by authentication with each equipment and STB1020 will be Ksb, Ksc, and Ksd, if it says in above sequence.
[0016] The content of authentication and key exchange is described [in / next / the above configuration] briefly. In addition, on these descriptions, a series of activities including an activity until it generates the subkey Ksx as a result of formation of authentication, and the activity of a transfer and acceptance of a control key Kc done after that shall be summarized, and it shall be called authentication and key exchange.
[0017] For example, when performing AV data transfer demand from VTR equipment (A) 1030 to STB1020, in advance of the activation, the following complicated authentications are needed.
[0018] Step 1001: That is, first, the authentication means 1032 of VTR equipment (A) 1030 generates random numbers A1 and A2, and enciphers this with the secrecy function Sa. Here, the enciphered random number is indicated to be Sa (A1, A2). The authentication means 1032 transmits Sa (A1, A2) and the self identification number IDa to STB1020 through the data transfer means 1031. Here, the identification number is beforehand given by the number of each terminal unit proper.
[0019] Step 1002: In STB1020, through the data transfer means 1024, the authentication means 1023 obtains Sa (A1, A2) and an identification number IDa,

recognizes the identification number, and chooses the secrecy function Sa corresponding to it from two or more held secrecy functions. Thereby, the secrecy function which STB1020 should use for authentication between VTR equipment (A) 1030 is specified.

[0020] Step 1003:, next the authentication means 1023 of STB1020 decode Sa (A1, A2) which carried out [above-mentioned] reception using the secrecy function Sa, restore A1 and A2, and only the latter random number A2 is returned to VTR equipment (A) 1030, without enciphering.

Step 1004:, next the authentication means 1032 of VTR equipment (A) 1030 compare the random number A2 returned from STB1020 with the random number A2 which oneself generated at the above-mentioned step 1001. If both random numbers are in agreement, it can be judged that STB1020 is equipment of normal.

[0021] Step 1005:, next the authentication means 1023 by the side of STB1020 generate a random number B1 and B-2, and encipher this with the secrecy function Sa. And Sa (B1, B-2) is transmitted to VTR equipment (A) 1030.

[0022] Step 1006: With VTR equipment (A) 1030, the authentication means 1032 decodes Sa (B1, B-2) which carried out [above-mentioned] reception using the secrecy function Sa, restores B1 and B-2, and return only latter random-number B-2 to STB1020, without enciphering.

[0023] Random-number B-2 to which step 1007:, next the authentication means 1023 have been returned from VTR equipment (A) 1030 is compared with random-number B-2 which oneself generated at the above-mentioned step 1005. If both random numbers are in agreement, it can be judged that VTR equipment (A) 1030 is normal equipment.

[0024] By the above, it means that authentication was materialized and both sides can check that partner equipment is equipment of normal mutually. Consequently, AV data transfer to VTR equipment (A) 1030 is permitted.

[0025] Four random numbers A1, A2, and B1 and B-2 have occurred for the authentication means 1023 and 1032 of both equipments as a result of this authentication.

[0026] Then, next, both authentication means 1023 and 1032 use random numbers A1 and B1, and generate the above-mentioned subkey Ksa, respectively. In addition, since not using a random number A2 and B-2 has the circumstances where these were transmitted without enciphering, on the occasion of generation of the subkey Ksa, those who use the random numbers A1 and B1 without such circumstances are because it sees from the safety of a key and excels more.

[0027] With the encryption means 1022, using the subkey Ksa generated by carrying out in this way, a control key Kc is enciphered and the work-piece key Kw is enciphered using a control key Kc. These are sent to the authentication means 1023. Moreover, it is enciphered by the work-piece key Kw, and AV data are sent to the data transfer means 1024.

[0028] And the control key Ksa (Kc) by which encryption was carried out [above-mentioned], and the enciphered work-piece key Kc (Kw) are transmitted to VTR equipment (A) 1030 through the data transfer means 1024 from the authentication means 1023. Then, the enciphered AV data Kw (AV) are transmitted to VTR equipment (A) 1030 from the data transfer means 1024.
[0029] On the other hand, with VTR equipment (A) 1030, the decryption means 1033 decodes the enciphered control key Ksa (Kc) first using the subkey Ksa obtained from the authentication means 1032. Next, the work-piece key Kc (Kw) enciphered using the decoded control key Kc is decoded. Furthermore, the enciphered AV data Kw (AV) are decoded using the work-piece key Kw decoded by carrying out in this way.
[0030] In addition, the work-piece key Kw which STB1020 uses is periodically changed during data transfer, in order to secure the safety of transfer data.
[0031] Therefore, the new work-piece key Kw enciphered whenever the work-piece key Kw was changed is sent to the terminal unit under data transfer from STB1020.
[0032]
[Problem(s) to be Solved by the Invention] However, in the way of such conventional data transfer, since the work-piece key Kw enciphered by the control key Kc will also be temporarily decoded supposing a control key Kc is decoded by the inaccurate person, it had the technical problem that enciphered AV data would be decoded by the inaccurate person as a result.
[0033] In this case, as part of authentication and key exchange, since a control key Kc is transmitted, if a control key Kc is only merely updated, it is necessary to perform actuation of authentication and key exchange at every updating conventionally, although it is possible to update a control key Kc, as mentioned above.
[0034] However, if actuation of authentication and key exchange is again performed at every renewal of Kc, processing of a up Norikazu ream until it generates a new subkey etc. will serve as a big burden for both equipments. Then, an invention-in-this-application person used to consider improving the security of a control key Kc by updating a control key Kc, without increasing the burden by actuation of authentication and key exchange on parenchyma compared with the former.
[0035] This invention aims at offering the data source which can raise the dependability about the nondisclosure of a control key Kc further compared with the former, a data sink, and a medium in consideration of the technical problem mentioned above, without increasing the burden on operation compared with the former.
[0036]
[Means for Solving the Problem] A transfer-request reception means by which this invention according to claim 1 receives the data transfer demand from a data sink, A data transfer means to perform a data transfer to said data sink based on said transfer request, A 1st encryption means to encipher said data transmitted based on the predetermined work-piece key Kw, A 2nd encryption means to encipher based on a control key Kc and to send the work-piece key Kw to said data sink, A secrecy

element generating means to generate the secrecy element used for generation of said control key Kc, All or a part of control keys Kc generated in the past, and said generated secrecy element, It has a control-key generation means to generate the new control key Kc, using the 1st function which makes them a variable. When said control key Kc is newly updated, it is the data source which is what transmits said secrecy element to said data sink which has said 1st function.

[0037] A transfer-request reception means by which this invention according to claim 2 receives the data transfer demand from a data sink, A data transfer means to perform a data transfer to said data sink based on said transfer request, A 1st encryption means to encipher said data transmitted based on the predetermined work-piece key Kw, A 2nd encryption means to encipher based on a control key Kc and to send the work-piece key Kw to said data sink, A control-key generation means to generate the new control key Kc, All or a part of control keys Kc generated in the past, and said newly generated control key Kc, When it has a secrecy element generation means to generate a secrecy element, using the 2nd function which makes them a variable and said control key Kc is newly updated, it is the data source which is what transmits said secrecy element to said data sink which has the inverse function of said 2nd function.

[0038] A transfer-request means by which this invention according to claim 3 gives a data transfer demand to the data source according to claim 1 or 2, While decoding the enciphered work-piece key Kw which is transmitted from said data source based on said transfer request by the control key Kc A decryption means to decode the enciphered data based on the work-piece key Kw, A hysteresis information storage means to memorize said control key Kc already used for decode of said work-piece key Kw as hysteresis information, A function storing means to store said the 1st function or said inverse function, and said the 1st function or inverse function stored, All or part of past control keys Kc memorized by said hysteresis information storage means It is the data sink equipped with a control-key generation means to generate the new control key Kc, based on said secrecy element transmitted from said data source according to claim 1 or 2.

[0039] This invention according to claim 11 is the medium which recorded the program for making a computer perform above any or all or a part of means of each means of one publication.

[0040]

[Embodiment of the Invention] Below, the gestalt of operation of this invention is explained with reference to a drawing.

[0041] (Gestalt of the 1st operation) Drawing 1 is the block diagram showing the configuration of the data source in the gestalt of 1 operation of this invention, and a data sink, and it describes the configuration of the gestalt of this operation, referring to this drawing below. In addition, with the gestalt of this operation, the same sign was fundamentally given to the thing of the same configuration, and the detailed

explanation was abbreviated to what was explained by drawing 6 .
[0042] drawing 1 -- being shown -- STB -- 100 -- **** -- already -- having stated -- drawing 6 -- the same -- a data sink -- equipment -- ****** -- VTR -- equipment -- (-- a --) -- 200 -- VTR -- equipment -- (-- b --) -- 300 -- a recording device -- (-- c --) -- 400 -- and -- TV -- equipment -- (-- d --) -- 500 -- connecting -- having -- **** -- a configuration -- it is . In addition, in drawing 1 , only VTR equipment (a) 200 was indicated as a terminal unit on account of explanation, and the publication of other terminal units was omitted. these -- a publication -- having omitted -- a terminal unit -- 300 - 500 -- the following -- stating -- VTR -- equipment -- (-- a --) -- 200 -- a configuration -- bases -- a target -- being the same -- a configuration -- having -- **** .
[0043] In this drawing, the configuration of STB100 is described first.
[0044] That is, the encryption means 101 is a means to encipher AV data from the receiving means 1021 by the work-piece key Kw. The transmitting-side authentication means 102 is a means to perform authentication and key exchange between terminal units. Moreover, the transmitting-side authentication means 102 is a means by which generate a subkey in authentication actuation and only the first time enciphers two or more control keys Kc using the generated subkey. Kc generating function selection means 103 are m functions of f1-fm, and a means to build in beforehand the function identifier 1 corresponding to it - m, and to choose any one function fi, in order to generate a control key Kc. Moreover, Kc generating function selection means 103 is a means to output the selected function fi to Kc generation means 106, and to output the function identifier i which corresponds to the transmitting-side authentication means 102. The random-number-generation means 104 is a means to generate and output random-number Kc' used for generation of a control key Kc. Kc storage means 105 is a means to memorize the already generated control key Kc. Kc generation means 106 is a means to generate the new control key Kc using some control keys [a part of] Kc which is sent from Kc storage means 106 and which were generated in the past, random-number Kc' by which the output was carried out [above-mentioned], and the function fi which makes them a variable and by which the output was carried out [above-mentioned]. Here, a part of control key Kc used as the variable of Function fi is a key generated before one and two with the gestalt of this operation. In addition, about this function, it mentions later further. Kw encryption means 107 is a means to encipher the work-piece key Kw using the generated control key Kc.
[0045] Since a control key Kc is updated one after another, it shall express the control key used first as Kc [1] in the gestalt of this operation on the occasion of initiation of data transfer, and shall express the control key used for the n-th as Kc [n] in it as a result of updating. Moreover, the random number similarly used in order to generate Kc [n+1] shall be expressed as Kc' [n]. However, n is taken as the natural number.

[0046] Therefore, the gestalt of this operation can express the above-mentioned function fi by the following formulas (several 1).
[0047]
[Equation 1] fi(Kc'[n],Kc[n-1],Kc[n])
Here, n is taken as the natural number.
[0048] Therefore, the control key Kc [n+1] generated by the n+1st can be expressed with the following formula (several 2).
[0049]
[Equation 2] Kc[n+1]=fi(Kc'[n],Kc[n-1],Kc[n])
Here, n is taken as the natural number.
[0050] In addition, the transfer-request reception means of this invention is a means including the data transfer means 1024 and the transmitting-side authentication means 102. Moreover, the data transfer means of this invention is a means including the data transfer means 1024 and the encryption means 101. The 1st encryption means of this invention is equivalent to the encryption means 101, and the 2nd encryption means is equivalent to Kw encryption means 107 again. The secrecy element generating means of this invention is equivalent to the random-number-generation means 104, and the 1st function of this invention is equivalent to Function fi. Moreover, the transmitting-side authentication means 102 has the secrecy function (Sa, Sb, Sc, Sd, ..., Sx) like the authentication means 1023 stated by drawing 6 .
[0051] Next, the configuration of VTR equipment 200 is described.
[0052] That is, in this drawing, the authentication demand means 201 is a means to perform an authentication demand, in order to require data transfer from STB100. The receiving-side authentication means 202 is a means to perform authentication and key exchange between STBs100. Moreover, the receiving-side authentication means 202 is a means which generates a subkey in authentication actuation and is sent as a result of authentication actuation to decode two or more enciphered control keys Kc by the subkey, and to extract a control key Kc [1] and to output to Kw decode means 203 out of the decode result. Moreover, the receiving-side authentication means 202 is a means which receives the enciphered work-piece key Kw and is sent to Kw decode means 203. Furthermore, the receiving-side authentication means 202 is a means to output the function identifier i sent from STB100 to Kc generating function selection means 204, and to output random-number Kc' [n] to Kc generation means 205 again again.
[0053] The decryption means 206 is a means to decode enciphered AV data which have been transmitted from STB100 using the work-piece key Kw, and to output to record / playback means (graphic display abbreviation) 1034. Kc generating function selection means 204 is a means to build in beforehand the same function as two or more above-mentioned functions which STB100 builds in, to extract the function fi corresponding to the inputted function identifier i, and to output to Kc generation means 205. This function fi can be expressed with several 1. Kc generation means 205

is a means to generate the new control key Kc as a variable of Function fi using the control key Kc which was being used before [one and two] reading from Kc hysteresis storage means 207, and random-number Kc' outputted from the receiving-side authentication means 202. This new Kc can be expressed with several 2. Moreover, Kc hysteresis storage means 207 is a means to memorize the hysteresis of the control key Kc generated by Kc generation means 205. In addition, when VTR equipment 200 receives a data transfer in the midst to which the data transfer has already been performed from the middle between STB100 and other terminal units, Kc hysteresis storage means 207 is a means to perform the following exceptional actuation. That is, it is a means to memorize reception and them for the control key which is using Kc hysteresis storage means 207 actually between terminal units besides the above, and the control key which was being used before one of them from STB100 in that case.

[0054] In addition, the receiving-side authentication means 202 has the secrecy function Sa like the authentication means 1032 stated by drawing 6 .

[0055] Actuation of the gestalt of this operation is explained [in / next / the above configuration], referring to drawing 1 and drawing 2 .

[0056] Here, the case where (1) STB100 starts AV data transfer only to VTR equipment 200 is described first, and it explains working [(2) above (1)] after that focusing on the case where the data transfer to another accepting-station equipment 400, i.e., recording apparatus, is started.

[0057] (1) Describe the case where AV data are transmitted, from STB100 only to VTR equipment 200 here as mentioned above.

[0058] In order for VTR equipment 200 to have desired AV data transmitted from STB100, after operating the authentication and key exchange same between STB100 and VTR equipment 200 as drawing 6 described, characteristic actuation of the gestalt of this operation is performed.

[0059] The demand of initiation of actuation of authentication and key exchange is performed by the authentication demand means 201 to STB100 at step 101:, i.e., here. Since the detail of actuation of subsequent authentication and key exchange is the same as that of what was stated at steps 1001-1007 mentioned above except for the following points, the explanation is omitted. In addition, in actuation of this authentication and key exchange, the receiving-side authentication means 202 performs generating of the random numbers A1 and A2 in VTR equipment 200, and the random-number-generation means 104 performs generating of the random number B1 in STB100, and B-2. Moreover, in actuation of the above-mentioned steps 1001-1007, in both equipments, the subkey Ksa is generated as drawing 6 described, when authentication was materialized. As step 102 describes the key first transmitted to VTR equipment 200 in subsequent actuation of authentication and key exchange with the gestalt of this operation, it is two pieces, and this point differs from the former.

[0060] Step 102:, i.e., two random numbers generated with the random-number-generation means 104, is defined as a dummy key Kc [0] and a control key Kc [1]. This dummy key Kc [0] and a control key Kc [1] are sent to the transmitting-side authentication means 102. Moreover, a control key Kc [1] is sent also to Kw encryption means 107.
[0061] That is, in this case, several 2 shall not be used about generation of Kc [0] and Kc [1], but the random number generated by the random-number-generation means 104 shall be used as exceptional treatment.
[0062] Step 103: These two keys Kc [0] and Kc [1] are further memorized by Kc storage means 105. Moreover, the function fi chosen by Kc generating function selection means 103 is sent to Kc generation means 106, and the function identifier i corresponding to it is sent to the transmitting-side authentication means 102. In addition, Function fi may be updated if needed.
[0063] Step 104: With the transmitting-side authentication means 102, it is enciphered by the subkey Ksa and the dummy key Kc [0] and control key Kc [1] which have been sent as mentioned above are sent to the data transfer means 1024 as Ksa (Kc [0], Kc [1]). Furthermore, Ksa (Kc [0], Kc [1]) is transmitted to VTR equipment 200 from the data transfer means 1024. In drawing 2 , the sign 601 was given to this transfer. Here, drawing 2 is the mimetic diagram from STB100 to the accepting-station equipment 200,400 performed with renewal of a control key shown focusing on the situation of a transfer. In this drawing, an axis of ordinate is time amount and time amount has passed towards the bottom since on in drawing.
[0064] In addition, the function identifier i corresponding to the Kc generating function fi is transmitted to VTR equipment 200 in the case of this transfer 601.
[0065] Step 105: Ksa (Kc [0], Kc [1]) and the function identifier i which have been transmitted from STB100 are sent to the receiving-side authentication means 202 by the data transfer means 1031.
[0066] Step 106: and the receiving-side authentication means 202 decode Ksa (Kc [0], Kc [1]), extract Kc [1] arranged back and send it to Kw decode means 203 as beforehand set between two keys arranged forward and backward. Moreover, the receiving-side authentication means 202 sends the function identifier i to Kc generating function selection means 204. And Kc generating function selection means 204 extracts the function fi corresponding to the identifier i, and sends to Kc generation means 205. In addition, both, through Kc generation means 205, decoded Kc [0] and Kc [1] are sent to Kc hysteresis storage means 207, and are memorized.
[0067] step 107: -- on the other hand -- Kw encryption means 107 -- a control key Kc -- [the work-piece key enciphered using 1], Kc[1 [i.e.,],] (Kw) should pass the transmitting-side authentication means 102 and the data transfer means 1024 -- it is transmitted to VTR equipment 200.
[0068] Step 108: Kc[1] (Kw) sent to VTR equipment 200 is sent to Kw decode means 203 through the receiving-side authentication means 202. Using the control key Kc

[1] sent in step 106, Kw decode means 203 decodes Kc[1] (Kw), and sends Kw to the decryption means 206.
[0069] Step 109: On the other hand, a transfer of Kw (AV) which is AV data enciphered by the encryption means 101 of STB100 is started through the data transfer means 1024.
[0070] Step 110: Kw (AV) is sent to the decryption means 206 from the data transfer means 1031. Using Kw sent from Kw decode means 203, the decryption means 206 decodes Kw (AV) and outputs it to record / playback means.
[0071] Next, in step 110, actuation in case a control key Kc is updated is described while decoded AV data being outputted to record / playback means.
[0072] Step 201: With the gestalt of this operation, a control key shall be updated periodically and the random-number-generation means 104 generates random-number Kc' periodically. That is, random-number Kc' [1] used for the 1st updating is sent to Kc generation means 106 and the transmitting-side authentication means 102 from the random-number-generation means 104.
[0073] Step 202: Random-number Kc' [1] sent to the transmitting-side authentication means 102 is transmitted to VTR equipment 200 through the data transfer means 1024. In drawing 2 , the sign 602 was given to this transfer.
[0074] Step 203: Kc generation means 106 reads Kc [0] memorized by Kc storage means 105 and Kc [1], and they are used for it as a variable of Function fi (several 2 reference) with random-number Kc' [1] sent from the random-number-generation means 104.
[0075] In this case, the new control key Kc [2] generated can be expressed as Kc[2] =fi (Kc' [1], Kc [0], Kc [1]) from several 2. In addition, Kc [2] is memorized by Kc storage means 105.
[0076] Step 204: The new control key Kc [2] is sent to Kw encryption means 107, and is used for encryption of the work-piece key Kw. Kc[2] (Kw) which is the enciphered work-piece key is transmitted to VTR equipment 200 like step 107.
[0077] Step 205: Random-number Kc' transmitted to VTR equipment 200 in step 202 again [1] It is sent to the receiving-side authentication means 202 from the data transfer means 1031, and is further sent to Kc generation means 205.
[0078] Step 206: With Kc generation means 205, read with Kc [0] memorized by Kc hysteresis storage means 207 and Kc [1], and use as a variable of Function fi (several 2 reference) with random-number Kc' [1] sent in step 205. In this case, the new control key Kc [2] generated is the same as what was stated at step 203, and can be expressed as Kc[2] =fi (Kc' [1], Kc [0], Kc [1]). In addition, Kc [2] is memorized by Kc hysteresis storage means 207.
[0079] Step 207: The new control key Kc [2] is sent to Kw decode means 203, and is used for decode of the work-piece key Kw enciphered by Kc [2]. The decoded work-piece key Kw is sent to the encryption decode means 206.
[0080] Step 208: The same actuation as step 110 is performed.

[0081] Next, in step 208, a control key Kc [2] describes the actuation in the case of being updated further while decoded AV data being outputted to record / playback means. Here, since there are many the same points as the already described content, only the focus about several 2 is described.
[0082] That is, the control key Kc [3] generated here can be expressed as follows by substituting 2 for several 2 n. In drawing 2 , the sign 603 was given to the transfer of random-number Kc' [2].
[0083]
[Equation 3]
Kc[3]=fi(Kc'[2],Kc[1],Kc[2])
The above (several 3), in the gestalt of this operation, the control key generated after the 2nd updating is generated by the control key used before one and two, random-number Kc' generated by the random-number-generation means 104 at every updating, and the function fi which makes them a variable so that clearly from reaching (several 2).
[0084] The dependability of a control key can be further raised by updating a control key using the hysteresis and the random number of the control key which was described above and which was used in the past, without repeating authentication actuation like according to the gestalt of this operation.
[0085] (2) In actuation of the above (1), after 2nd renewal of a control key is performed, describe the case where the data transfer to a recording apparatus 400 is started, referring to drawing 2 .
[0086] Step 301: The same authentication actuation as step 101 is performed between STB100 and the recording device 400 which newly performs a transfer request.
[0087] Step 302: After authentication is materialized, the transmitting-side authentication means 102 reads the control key Kc present in use [3] currently recorded on Kc storage means 105, and the control key Kc [2] which was being used before one of them, and enciphers it by the subkey Ksc. And the function identifier i corresponding to this Ksc (Kc [2], Kc [3]) and the function fi present in use is transmitted to a recording device 400 through the data transfer means 1024 (in drawing 2 , the sign 604 was given to this transfer). In addition, the subkey Ksc is generated by the above-mentioned authentication actuation by the same approach as the above.
[0088] Step 303: In a recording device 400, the receiving-side authentication means 202 decodes Ksc (Kc [2], Kc [3]) sent as mentioned above using the subkey Ksc, and extracts Kc [3]. Actuation of this decode and extract and actuation of subsequent Kc generating function selection means 204, Kc hysteresis storage means 207, etc. are the same as the content stated at step 106.
[0089] step 304: -- on the other hand -- STB100 -- Kw encryption means 107 -- the control key Kc current in use -- [Kc[3 (Kw) which enciphered the work-piece key

Kw using 3]] is transmitted to a recording device 400. This Kc[3] (Kw) is the same as what was transmitted to VTR equipment 200.
[0090] Step 305: Decode actuation of Kc[3] (Kw) with a recording device 400 is the same as the content of step 108.
Step 306: Enciphered AV data transfer actuation is the same as the content of step 109.
[0091] Step 307: Decode actuation of AV data with a recording apparatus 400 is the same as the content of step 110.
[0092] Next, actuation in case a control key Kc [3] is updated is the same as what read Kc [0] as Kc [2], and read Kc [1] as Kc [3], and read random-number Kc' [1] as random-number Kc' [3] in explanation at the above-mentioned steps 201-208.
[0093] The control key Kc [4] generated here can be expressed as follows by substituting 3 for several 2 n. In drawing 2 , the sign 605 was given to the transfer of random-number Kc' [3].
[0094]
[Equation 4]
Kc[4]=fi(Kc'[3],Kc[2],Kc[3])
Thus, even if the terminal unit which receives AV data transfer from the middle appears and an accepting station increases, the control key which STB100 uses becomes what was common regardless of the number of accepting-station equipment.
[0095] Even if an inaccurate person solves by this any one of the control keys used so far for example, by round robin count etc. by chance, since a control key is generated by combination with another random number, the hysteresis of the control key till then and it can prevent with it that the control key generated after the control key by which unjust decode was carried out will be solved continuously.
[0096] Moreover, if the hysteresis of the control key before it is not known even if random-number Kc' used for renewal of a control key is monitored by the inaccurate person, decode of a control key is impossible.
[0097] In addition, although the gestalt of the above-mentioned implementation described the case where Function fi (the 1st function) generated the new control key Kc, using the random number generated previously and the past control key Kc, it is good also as the data source of not only this but the configurations following for example. that is, specifically, it is shown in drawing 3 -- as -- the above-mentioned Kc generation means 106 -- replacing with -- (1) -- with a control-key generation means 1106 to generate the new control key Kc All or a part of control keys Kc which replaced with the above-mentioned random-number-generation means 104, and was generated in the (2) past, and said newly generated control key Kc, It has a secrecy element generation means 1104 to generate secrecy element Kc', using the 2nd function Fi which makes them a variable. When said control key Kc is newly updated, you may be the data source 1100 of a configuration of transmitting said secrecy element Kc' to the data sink 1200 which has inverse function F-1i of said 2nd

function. On the other hand, as shown in a data sink 1200 at drawing 3 , the inverse function selection means 1204 equipped with the inverse function corresponding to two or more 2nd functions which the 2nd function selection means 1103 has is established. This inverse function selection means 1204 obtains the function identifier i from the receiving-side authentication means 202, chooses inverse function F-1i corresponding to it, and sends it to Kc generation means 205. Kc generation means 205 generates the new control key Kc like the above using sent inverse function F-1i by making the control key Kc of secrecy element Kc' from the receiving-side authentication means 202, and the past into a variable.

[0098] Moreover, although the case where the control key Kc [1] first used for encryption of the work-piece key Kw and the key Kc [0] used for renewal of the control key were enciphered and transmitted by the first-time transfer 601 (refer to drawing 2) was stated with the gestalt of the above-mentioned implementation when authentication was materialized Not only in this, for example, the 1st function which a data sink has (For example, function fi) Or in the stage when it runs short of that the variable of the above-mentioned inverse function F-1i generates a control key Kc, you may be the data source of a configuration of transmitting to said data sink by making coding information containing said control key Kc into initial information. That is, as shown in drawing 4 , specifically, STB2100 transmits Ksa (Kc [1], Kc [2]) in transfer 1602. Since the subkey Ksa generated in the transfer 1602 by the authentication and key exchange already performed is used as it is, generation of a new subkey is unnecessary. The VTR equipment 2200 as a data sink decodes transmitted Ksa (Kc [1], Kc [2]), and extracts Kc [2].

[0099] Moreover, the 1st function fi which a data sink has, or the variable of the above-mentioned inverse function F-1i may be the data source of a configuration of transmitting to said data sink by making said variable containing a secrecy element (for example, random-number Kc') which run short into initial information as an example different from this in the stage when generating a control key Kc runs short of. That is, if the case where (several 2) of the gestalt of the above-mentioned implementation is used is specifically described as shown in drawing 5 for example, the control key Kc which can be expressed by the following formula (several 5) will be generated in both equipments using Function fi.

[0100]

[Equation 5]

Kc[1]=fi(Kc'[0],Kc[-1],Kc[0])

Here, Kc' [0] is secrecy elements, such as a random number generated with the data source, and Kc [-1] and Kc [0] are intact control keys till then. These intact control keys may make it generate as a random number, and may be beforehand extracted out of the plurality built in. In this case, it is necessary to the VTR equipment 3200 as a data sink to encipher by the subkey and to transmit Kc' [0], Kc [-1], and Kc [0] as a variable required for generation of a control key Kc [1], from STB3100 as the data

source in the transfer 2601 shown in drawing 5 .
[0101] Moreover, it sets in the first half of (1) among the stages which want the variable of the 1st function which a data sink has as another example as be fastidious, or the above-mentioned inverse function for generating a control key Kc. You may be the data source of a configuration of transmitting to said data sink in the second half of the first stage by making said variable which contains said secrecy element in the second half of (2) in the first half of the first stage by making coding information containing said control key Kc into information and which run short into information. That is, it replaces with the transfer 601 of drawing 2 , and Ksa (Kc [1]) is specifically transmitted, it replaces with the transfer 602 of this drawing, and Kc' [1] as a secrecy element and Kc [0] as a variable which is carrying out [above-mentioned] lack are transmitted. Thereby, as a result of transfer 601, Kc [1] is extracted in a data sink and it is used as first control key. Moreover, in a data sink, Function fi generates the following control key Kc [2] by making into a variable the control key Kc [1] extracted by carrying out in this way, Kc' [1] which came to hand by transfer 602, and Kc [0].
[0102] Moreover, although it has two or more Kc generating functions beforehand and the case where it was used from the inside, choosing one was stated with the gestalt of the above-mentioned implementation, the configuration of transmitting the function itself used in the case for example, not only of this but authentication actuation may be used, or the function may be fixed from the start.
[0103] Moreover, although the gestalt of the above-mentioned implementation described the case where Function fi (the 1st function) generated the new control key Kc, using the random number generated previously and the past control key Kc Not only in this, for example, a control-key generation means to generate the new control key Kc, All or a part of control keys Kc generated in the past, and said newly generated control key Kc, When it has a secrecy element generation means to generate a secrecy element, using the 2nd function which makes them a variable and said control key Kc is newly updated, you may be the data source of a configuration of transmitting said secrecy element to the data sink which has the inverse function of said 2nd function.
[0104] Moreover, with the gestalt of the above-mentioned implementation, when generating the new control key Kc, the case where the thing in front of one and two was used as a variable was stated as hysteresis of a control key Kc, but as long as it is the control key used not only for this but for the past, anything is sufficient as before two, three or one, and three etc. Moreover, if it is the past control key Kc, even if not only two pieces but all the control keys used in the past if it was good without limit and storage capacity could be secured when it was one or more pieces are used for the number, it will not be cared about.
[0105] Moreover, a magnetic-recording medium, an optical recording medium, etc. which recorded the program for making a computer perform each means of any of the gestalt of the operation described above or one publication, the means of all or a part

of steps, or a step can be created, and the same actuation as the above can also be performed using this. The same effectiveness as the above is demonstrated also in this case.

[0106] Moreover, using a computer, each means of the gestalt of the above-mentioned implementation or processing actuation of a step may be realized by software by work of a program, or may realize the above-mentioned processing actuation in hard by circuitry characteristic [without using a computer].

[0107]

[Effect of the Invention] It has the advantage in which this invention can raise the dependability about the nondisclosure of a control key further compared with the former, without increasing the burden on parenchyma compared with the former so that clearly from the place described above.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The block diagram showing the configuration of the data source in the gestalt of 1 operation of this invention, and a data sink

[Drawing 2] The mimetic diagram shown in the gestalt of this operation focusing on the situation of the transfer to the accepting-station equipment performed with renewal of a control key from STB

[Drawing 3] The block diagram showing the configuration of the data source in the gestalt of other operations of this invention, and a data sink

[Drawing 4] The mimetic diagram shown in the gestalt of another operation of this invention focusing on the situation of the transfer to the accepting-station equipment performed with renewal of a control key from STB

[Drawing 5] The mimetic diagram shown in the gestalt of still more nearly another operation of this invention focusing on the situation of the transfer to the accepting-station equipment performed with renewal of a control key from STB

[Drawing 6] The block diagram showing the configuration of the conventional data source and a data sink

[Description of Notations]

100 STB

101 Encryption Means

102 Transmitting-Side Authentication Means

103 Kc Generating Function Selection Means

104 Random-Number-Generation Means

105 Kc Storage Means

106 Kc Generation Means
107 Kw Encryption Means

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－289327

(43)公開日　平成11年(1999)10月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ

審査請求　未請求　請求項の数11　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－89097

(22)出願日　平成10年(1998)４月１日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　西村　拓也
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　飯塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内

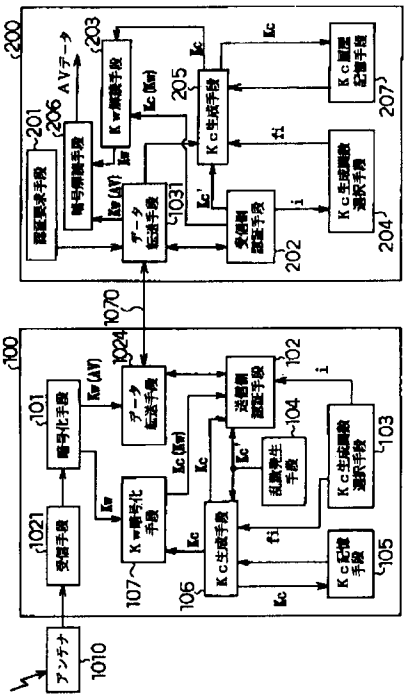
(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　データ送信装置、データ受信装置、及び媒体

(57)【要約】
【課題】コントロールキーＫｃが不正に解読されると、それで暗号化されているワークキーＫｗも解読されるため、ＡＶデータが不正に解読されるという課題。
【解決手段】ＳＴＢ１００は、受信手段１０２１からのＡＶデータをワークキーＫｗにより暗号化する暗号化手段１０１と、ＶＴＲ装置２００と認証動作を行い、Ｋｃの暗号化を行う送信側認証手段１０２と、Ｋｃを生成するために、複数個の関数とその関数識別子を予め内蔵し、何れかの関数を選択するＫｃ生成関数選択手段１０３と、Ｋｃを生成する際に利用する乱数Ｋｃ′を発生させる乱数発生手段１０４と、既に生成されたＫｃを記憶するＫｃ記憶手段１０５と、過去に生成されたＫｃの一部と、上記出力された乱数Ｋｃ′と、それらを変数とする上記選択された関数ｆｉとを利用して、新たなＫｃを生成するＫｃ生成手段１０６と、生成されたＫｃを用いてＫｗを暗号化するＫｗ暗号化手段１０７手段等を備える。



【特許請求の範囲】

【請求項１】　データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、
そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、
前記コントロールキーＫｃの生成に利用する秘密要素を発生させる秘密要素発生手段と、
過去に生成されたコントロールキーＫｃの全部又は一部と前記発生された秘密要素と、それらを変数とする第１の関数とを利用して、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備え、
前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第１の関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項２】　データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、
前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、
前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、
そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、
新たなコントロールキーＫｃを生成するコントロールキー生成手段と、
過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、
前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有する前記データ受信装置に転送するものであることを特徴とするデータ送信装置。

【請求項３】　請求項１又は２記載のデータ送信装置にデータ転送要求を行う転送要求手段と、
前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーＫｗを、コントロールキーＫｃで解読するとともに、暗号化されたデータを、そのワークキーＫｗに基づいて解読する暗号解読手段と、
前記ワークキーＫｗの解読に既に利用された前記コントロールキーＫｃを履歴情報として記憶する履歴情報記憶手段と、
前記第１の関数又は前記逆関数を格納する関数格納手段と、
前記格納されている第１の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーＫｃの全部又は一部と、請求項１又は２記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、を備えたことを特徴とするデータ受信装置。

【請求項４】　前記データ送信装置が別のデータ受信装置と既に前記データの転送を行っている途中から、データの転送を要求する場合、
前記コントロールキー生成手段により初期段階で利用される前記過去のコントロールキーＫｃは、前記履歴情報記憶手段に記憶されている前記コントロールキーＫｃではなく、前記データ送信装置から転送されてくるコントロールキーＫｃであることを特徴とする請求項３記載のデータ受信装置。

【請求項５】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、前記コントロールキーＫｃを含む暗号情報を初期情報として、前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項６】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、前記秘密要素を含む前記不足している変数を初期情報として前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項７】　前記転送を行う旨が決定された場合、
前記データ受信装置が有する前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前半においては、前記コントロールキーＫｃを含む暗号情報を初期前半情報として、又、（２）後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送することを特徴とする請求項１又は２記載のデータ送信装置。

【請求項８】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期においては、請求項５記載のデータ送信装置から転送されてくる前記初期情報を解読し、前記コントロールキーＫｃを抽出する抽出手段を備え、
前記暗号解読手段が、前記抽出されたコントロールキーＫｃを前記解読に利用することを特徴とする請求項３記載のデータ受信装置。

【請求項９】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している

時期においては、前記コントロールキー生成手段が、前記６記載のデータ送信装置から転送されてくる前記初期情報と、前記関数とを利用して、前記コントロールキーＫｃを生成することを特徴とする請求項３記載のデータ受信装置。

【請求項１０】　前記第１の関数又は前記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前記前半においては、請求項６記載のデータ送信装置から転送されてくる前記初期前半情報が解読され、前記コントロールキーＫｃが抽出され、又、（２）前記後半においては、請求項６記載のデータ送信装置から転送されてくる前記初期後半情報と前記関数とを利用して、前記コントロールキーＫｃが生成されることを特徴とする請求項３記載のデータ受信装置。

【請求項１１】　請求項１～１０の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録したことを特徴とする媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ送信装置、データ受信装置、及び媒体に関する。

【０００２】

【従来の技術】従来より、衛星放送で送られてくるテレビ番組等を、衛星放送受信機（以下、これを単に、ＳＴＢと呼ぶ）により受信して、その受信機に接続されたＶＴＲ装置で録画したり、テレビで視聴したりすることが行われている。

【０００３】この場合、放送されてくる映像・音声データの中には、記録が禁止されているものや、１回だけ記録可能とされている条件付きデータがある。従って、これらの条件が守られる為には、この条件を正しく認識して、正規に動作する装置をユーザ側が使用することが前提となる。

【０００４】そこで、ＳＴＢから、例えばＶＴＲ装置に対して、１回のみ記録可能なデータを送信する場合、先ず、そのＶＴＲ装置が、上記の様な正規なＶＴＲ装置であるかどうかを確認するための認証・鍵交換（ＡＫＥ）動作が行われるのが通常である。

【０００５】そして、この認証作業が成立しなかった場合には、認証対象となったＶＴＲ装置を不正装置であると認定し、その様な不正装置に対しては、データの送信を行わないようにする。

【０００６】以下、図６を参照しながら、従来のＳＴＢと各端末装置との構成と、その認証動作を中心に説明する。

【０００７】図６は、従来のＳＴＢと、ＶＴＲ装置等の各端末装置との接続状況及び構成を示すブロック図である。

【０００８】同図に示す様に、アンテナ１０１０は、衛星からの放送電波を受信する手段であり、ＳＴＢ１０２０は、受信した放送電波をＡＶデータに変換する手段である。データ伝送ライン１０７０は、ＳＴＢ１０２０と、以下に述べる各端末装置とを間に設けられたデータ伝送のためのバスラインである。又、端末装置として、ＶＴＲ装置（Ａ）１０３０、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｃ）１０５０、更にＴＶ装置（Ｄ）が、データ伝送ライン１０７０によりＳＴＢ１０２０と接続されている。

【０００９】次に、同図を参照しながら、ＳＴＢ１０２０の内部構成について更に述べる。

【００１０】即ち、受信手段１０２１は、アンテナ１０１０と直結し、受信したデータの復調を行い、その受信データに施されている放送用スクランブルを解除し、更に、多重化されている受信データを分離する手段である。暗号化手段１０２２は、予め備えた暗号化のためのワークキーＫｗにより、受信手段１０２１から出力されてきたＡＶデータを圧縮状態のまま暗号化する手段である。又、コントロールキーＫｃは、ＳＴＢ１０２０に予め内蔵されており、ワークキーＫｗを暗号化手段により暗号化するための鍵である。更に又、暗号化手段１０２２は、認証手段１０２３により、後述する認証動作の結果生成されたサブキーを用いてコントロールキーＫｃを暗号化する手段である。

【００１１】認証手段１０２３は、ＡＶデータの転送要求をしてきた端末装置との間で、双方の装置が正規の装置であるかどうかを互いに確かめ合うため、所定の秘密関数を利用して認証作業を行い、その結果として、認証相手に対応したサブキーＫｓａを生成する手段である。又、認証手段１０２３は、あらゆる端末装置が有する固有の全ての秘密関数（Ｓａ，Ｓｂ，Ｓｃ，Ｓｄ，・・，Ｓｎ，・・・）を、それらの識別番号と対応させて保有している。データ転送手段１０２４は、ディジタル・インタフェースとして知られているＩＥＥＥ１３９４である。データ転送手段１０２４は、リアルタイム性の保証が必要となる映像や音声の様なデータの転送に適したアイソクロナス転送と、その必要のない認証用データやコマンド等の転送に適したアシンクロナス転送の２つの転送を行う手段である。尚、上記暗号化されたＡＶデータは、暗号化手段１０２２からデータ転送手段１０２４へ送られる。又、上記暗号化されたワークキーや、暗号化されたコントロールキーは、認証手段１０２３からデータ転送手段１０２４へ送られる。

【００１２】尚、暗号化されたＡＶデータＫｗ（ＡＶ）、暗号化されたワークキーＫｃ（Ｋｗ）、そして暗号化されたコントロールキーＫｓａ（Ｋｃ）は、データ転送手段１０２４からＶＴＲ装置１０３０等の端末装置に送られる。

【００１３】次に、ＶＴＲ装置（Ａ）１０３０の内部構成について、更に述べる。

【００１４】同図に示すとおり、データ転送手段１０３

１は、データ転送手段１０２４と同様の手段であり、暗号化されたワークキー及び暗号化されたＡＶデータを受け取る手段である。認証手段１０３２は、固有の秘密関数Ｓａを予め有しており、認証作業の結果として、サブキーＫｓａを生成して、復号化手段１０３３へ出力する手段である。復号化手段１０３３は、データ転送手段１０３１から得た暗号化されたコントロールキーＫｓａ（Ｋｃ）をサブキーＫｓａにより復号し、この復号化されたコントロールキーＫｃにより、暗号化されたワークキーＫｃ（Ｋｗ）を復号し、その復号化されたワークキーＫｗにより、暗号化されたＡＶデータＫｗ（ＡＶ）を復号する手段である。記録・再生手段１０３４は、復号化されたＡＶデータを記録し、又、その記録データを再生する手段である。

【００１５】尚、その他の端末装置である、ＶＴＲ装置（Ｂ）１０４０、記録装置（Ｄ）１０５０、ＴＶ装置（Ｄ）１０６０も、記録・再生手段を除き、上記ＶＴＲ装置（Ａ）１０３０の構成と基本的に同じである。但し、各認証手段が予め有する秘密関数は、上記各装置の順番でいえば、Ｓｂ、Ｓｃ、Ｓｄである。従って、各装置と、ＳＴＢ１０２０との認証作業により生成されるサブキーは、上記の順番でいえば、Ｋｓｂ、Ｋｓｃ、Ｋｓｄである。

【００１６】以上の構成において、次に、認証・鍵交換の内容を簡単に述べる。尚、本明細書では、認証の成立の結果としてサブキーＫｓｘを生成するまでの作業、及びその後に行うコントロールキーＫｃの転送・受理の作業を含む一連の作業をまとめて、認証・鍵交換というものとする。

【００１７】例えば、ＶＴＲ装置（Ａ）１０３０からＳＴＢ１０２０に対して、ＡＶデータの転送要求を行う場合、その実行に先立ち次のような複雑な認証作業が必要となる。

【００１８】ステップ１００１：即ち、先ず、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、乱数Ａ１，Ａ２を発生させ、これを秘密関数Ｓａにより暗号化する。ここで、暗号化された乱数をＳａ（Ａ１，Ａ２）と記載する。認証手段１０３２は、Ｓａ（Ａ１，Ａ２）と自己の識別番号ＩＤａとをデータ転送手段１０３１を介して、ＳＴＢ１０２０へ転送する。ここで、識別番号は、各端末装置固有の番号で予め与えられている。

【００１９】ステップ１００２：ＳＴＢ１０２０では、認証手段１０２３がデータ転送手段１０２４を介して、Ｓａ（Ａ１，Ａ２）と識別番号ＩＤａとを得て、その識別番号を認識して、それに対応する秘密関数Ｓａを、保有している複数の秘密関数の中から選択する。これにより、ＳＴＢ１０２０が、ＶＴＲ装置（Ａ）１０３０との間で認証に使用すべき秘密関数が特定される。

【００２０】ステップ１００３：次に、ＳＴＢ１０２０の認証手段１０２３が、秘密関数Ｓａを用いて、上記受信したＳａ（Ａ１，Ａ２）を解読し、Ａ１，Ａ２を復元して、後者の乱数Ａ２のみを、暗号化せずにＶＴＲ装置（Ａ）１０３０へ送り返す。

ステップ１００４：次に、ＶＴＲ装置（Ａ）１０３０の認証手段１０３２が、ＳＴＢ１０２０から送り返されてきた乱数Ａ２と、自らが、上記ステップ１００１で発生させた乱数Ａ２とを比較する。双方の乱数が一致すれば、ＳＴＢ１０２０が正規の装置であると判断出来る。

【００２１】ステップ１００５：次に、ＳＴＢ１０２０側の認証手段１０２３が、乱数Ｂ１，Ｂ２を発生させ、これを秘密関数Ｓａにより暗号化する。そして、Ｓａ（Ｂ１，Ｂ２）をＶＴＲ装置（Ａ）１０３０へ転送する。

【００２２】ステップ１００６：ＶＴＲ装置（Ａ）１０３０では、認証手段１０３２が秘密関数Ｓａを用いて、上記受信したＳａ（Ｂ１，Ｂ２）を解読し、Ｂ１，Ｂ２を復元して、後者の乱数Ｂ２のみを、暗号化せずにＳＴＢ１０２０へ送り返す。

【００２３】ステップ１００７：次に、認証手段１０２３が、ＶＴＲ装置（Ａ）１０３０から送り返されてきた乱数Ｂ２と、自らが、上記ステップ１００５で発生させた乱数Ｂ２とを比較する。双方の乱数が一致すれば、ＶＴＲ装置（Ａ）１０３０が正規装置であると判断出来る。

【００２４】以上により、認証が成立したことになり、双方が互いに相手装置が正規の装置であることを確認出来る。その結果、ＶＴＲ装置（Ａ）１０３０へのＡＶデータの転送が許可される。

【００２５】この認証作業の結果、４つの乱数Ａ１，Ａ２とＢ１，Ｂ２が、双方の装置の認証手段１０２３，１０３２に発生している。

【００２６】そこで、次に、双方の認証手段１０２３，１０３２がそれぞれ、乱数Ａ１，Ｂ１を用いて上記サブキーＫｓａを生成する。尚、サブキーＫｓａの生成に際し、乱数Ａ２，Ｂ２を使用しないのは、これらは、暗号化せずに転送されたという経緯があるため、その様な経緯の無い乱数Ａ１，Ｂ１を使用する方が、キーの安全性から見て、より優れているからである。

【００２７】暗号化手段１０２２では、この様にして生成されたサブキーＫｓａを用いて、コントロールキーＫｃが暗号化され、又、コントロールキーＫｃを用いてワークキーＫｗが暗号化される。これらは、認証手段１０２３へ送られる。又、ＡＶデータはワークキーＫｗで暗号化されて、データ転送手段１０２４へ送られる。

【００２８】そして、上記暗号化されたコントロールキーＫｓａ（Ｋｃ）と、暗号化されたワークキーＫｃ（Ｋｗ）が、認証手段１０２３からデータ転送手段１０２４を介してＶＴＲ装置（Ａ）１０３０へ転送される。その後、暗号化されたＡＶデータＫｗ（ＡＶ）がデータ転送手段１０２４から、ＶＴＲ装置（Ａ）１０３０へ転送さ

れる。

【００２９】一方、ＶＴＲ装置（Ａ）１０３０では、復号化手段１０３３が、先ず、認証手段１０３２から得たサブキーＫｓａを用いて、暗号化されたコントロールキーＫｓａ（Ｋｃ）の復号を行う。次に、復号されたコントロールキーＫｃを用いて暗号化されたワークキーＫｃ（Ｋｗ）の復号を行う。更に、この様にして復号されたワークキーＫｗを用いて、暗号化されたＡＶデータＫｗ（ＡＶ）を復号するものである。

【００３０】尚、ＳＴＢ１０２０が、使用するワークキーＫｗは、転送データの安全性を確保するために、データ転送中において定期的に変更される。

【００３１】従って、ワークキーＫｗが変更される度に、暗号化された新たなワークキーＫｗが、ＳＴＢ１０２０からデータ転送中の端末装置へ送られる。

【００３２】

【発明が解決しようとする課題】しかしながら、このような従来のデータ転送のやり方では、仮に、コントロールキーＫｃが不正者によって解読されたとすると、コントロールキーＫｃで暗号化されているワークキーＫｗも解読されてしまうため、結果的に、暗号化されたＡＶデータが、不正者によって解読されることになるという課題を有していた。

【００３３】この場合、コントロールキーＫｃを更新することが考えられるが、上述したとおり、従来は、認証・鍵交換の一環として、コントロールキーＫｃを転送するものであるから、ただ単にコントロールキーＫｃを更新するとなると、認証・鍵交換の動作を更新の度に行う必要がある。

【００３４】しかし、認証・鍵交換の動作をＫｃの更新の度に再度行うとなると、新たなサブキーを生成するまでの上記一連の処理等が、双方の装置にとって大きな負担となる。そこで、本願発明者は、認証・鍵交換の動作による負担を従来に比べて実質上増やすことなく、コントロールキーＫｃを更新することにより、コントロールキーＫｃのセキュリティーを向上することを考えたものである。

【００３５】本発明は、上述した課題を考慮して、従来に比べて実施上の負担を増やすことなくコントロールキーＫｃの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るデータ送信装置、データ受信装置、及び媒体を提供することを目的とする。

【００３６】

【課題を解決するための手段】請求項１記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、前記コントロールキーＫｃの生成に利用する秘密要素を発生させる秘密要素発生手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記発生された秘密要素と、それらを変数とする第１の関数とを利用して、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第１の関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【００３７】請求項２記載の本発明は、データ受信装置からのデータ転送要求を受け付ける転送要求受付手段と、前記転送要求に基づいて、前記データ受信装置にデータの転送を行うデータ転送手段と、前記転送されるデータを所定のワークキーＫｗに基づいて暗号化する第１暗号化手段と、そのワークキーＫｗをコントロールキーＫｃに基づいて暗号化し、前記データ受信装置へ送る第２暗号化手段と、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有する前記データ受信装置に転送するものであるデータ送信装置である。

【００３８】請求項３記載の本発明は、請求項１又は２記載のデータ送信装置にデータ転送要求を行う転送要求手段と、前記転送要求に基づいて前記データ送信装置から転送されてくる暗号化されたワークキーＫｗを、コントロールキーＫｃで解読するとともに、暗号化されたデータを、そのワークキーＫｗに基づいて解読する暗号解読手段と、前記ワークキーＫｗの解読に既に利用された前記コントロールキーＫｃを履歴情報として記憶する履歴情報記憶手段と、前記第１の関数又は前記逆関数を格納する関数格納手段と、前記格納されている第１の関数又は逆関数と、前記履歴情報記憶手段に記憶されている過去のコントロールキーＫｃの全部又は一部と、請求項１又は２記載の前記データ送信装置から転送されてくる前記秘密要素とに基づいて、新たなコントロールキーＫｃを生成するコントロールキー生成手段とを備えたデータ受信装置である。

【００３９】請求項１１記載の本発明は、上記の何れか一つに記載の各手段の全部又は一部の手段をコンピュータに実行させるためのプログラムを記録した媒体である。

【００４０】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００４１】（第１の実施の形態）図１は、本発明の一

実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図であり、以下に、同図を参照しながら、本実施の形態の構成について述べる。尚、本実施の形態では、図６で説明したものと、基本的に同じ構成のものには、同じ符号を付し、その詳細な説明は省略した。

【００４２】図１に示すＳＴＢ１００には、既に述べた図６と同様に、データ受信端末装置としてＶＴＲ装置（ａ）２００、ＶＴＲ装置（ｂ）３００、記録装置（ｃ）４００及びＴＶ装置（ｄ）５００が接続されている構成である。尚、図１では、説明の都合上、端末装置としてＶＴＲ装置（ａ）２００のみを記載し、他の端末装置の記載を省略した。これら記載を省略した端末装置３００～５００は、以下に述べるＶＴＲ装置（ａ）２００の構成と基本的に同様の構成を備えている。

【００４３】同図において、先ず、ＳＴＢ１００の構成を述べる。

【００４４】即ち、暗号化手段１０１は、受信手段１０２１からのＡＶデータをワークキーＫｗにより暗号化する手段である。送信側認証手段１０２は、端末装置との間で認証・鍵交換を行う手段である。又、送信側認証手段１０２は、認証動作においてサブキーを生成し、初回のみ、その生成したサブキーを用いて複数個のコントロールキーＫｃを暗号化する手段である。Ｋｃ生成関数選択手段１０３は、コントロールキーＫｃを生成するために、f_1～f_mのm個の関数と、それに対応する関数識別子１～mを予め内蔵しており、何れか一つの関数f_iを選択する手段である。又、Ｋｃ生成関数選択手段１０３は、Ｋｃ生成手段１０６に対しては、選択した関数f_iを出力し、送信側認証手段１０２に対しては、対応する関数識別子ｉを出力する手段である。乱数発生手段１０４は、コントロールキーＫｃの生成に利用される乱数Ｋｃ′を発生し、出力する手段である。Ｋｃ記憶手段１０５は、既に生成されたコントロールキーＫｃを記憶する手段である。Ｋｃ生成手段１０６は、Ｋｃ記憶手段１０６から送られてくる、過去に生成された幾つかのコントロールキーＫｃの一部と、上記出力された乱数Ｋｃ′と、それらを変数とする上記出力された関数f_iとを利用して、新たなコントロールキーＫｃを生成する手段である。ここで、関数ｆｉの変数となるコントロールキーＫｃの一部とは、本実施の形態では、１つ前と、２つ前に生成したキーである。尚、この関数については、更に後述する。Ｋｗ暗号化手段１０７は、生成されたコントロールキーＫｃを用いてワークキーＫｗを暗号化する手段である。

【００４５】本実施の形態では、コントロールキーＫｃが、次々と更新されるので、データ転送の開始に際し、最初に使用されるコントロールキーをＫｃ[１]と表し、更新の結果、ｎ番目に使用されるコントロールキーをＫｃ[ｎ]と表すものとする。又、同様にして、Ｋｃ[ｎ＋１]を生成するために利用された乱数をＫｃ′[ｎ]と表すものとする。但し、ｎは、自然数とする。

【００４６】従って、本実施の形態では、上記関数ｆｉは、次のような式（数１）で表せる。

【００４７】

【数１】ｆｉ（Ｋｃ′[ｎ]，Ｋｃ[ｎ－１]，Ｋｃ[ｎ]）

ここで、ｎは、自然数とする。

【００４８】よって、ｎ＋１番目に生成されるコントロールキーＫｃ[ｎ＋１]は、次の式（数２）で表せる。

【００４９】

【数２】Ｋｃ[ｎ＋１]＝ｆｉ（Ｋｃ′[ｎ]，Ｋｃ[ｎ－１]，Ｋｃ[ｎ]）

ここで、ｎは、自然数とする。

【００５０】尚、本発明の転送要求受付手段は、データ転送手段１０２４及び送信側認証手段１０２を含む手段である。又、本発明のデータ転送手段は、データ転送手段１０２４及び暗号化手段１０１を含む手段である。本発明の第１暗号化手段は、暗号化手段１０１に、又、第２暗号化手段は、Ｋｗ暗号化手段１０７に対応する。本発明の秘密要素発生手段は、乱数発生手段１０４に対応し、本発明の第１関数は、関数f_iに対応する。また、送信側認証手段１０２は、図６で述べた認証手段１０２３と同様に、秘密関数（Ｓａ、Ｓｂ、Ｓｃ、Ｓｄ、・・・、Ｓｘ）を有している。

【００５１】次に、ＶＴＲ装置２００の構成について述べる。

【００５２】即ち、同図において、認証要求手段２０１は、ＳＴＢ１００に対して、データ転送の要求をするために認証要求を行う手段である。受信側認証手段２０２は、ＳＴＢ１００との間で認証・鍵交換を行う手段である。又、受信側認証手段２０２は、認証動作においてサブキーを生成し、認証動作の結果として送られてくる、暗号化された複数個のコントロールキーＫｃをそのサブキーにより解読し、その解読結果の中から、コントロールキーＫｃ[１]を抽出し、Ｋｗ解読手段２０３に出力する手段である。又、受信側認証手段２０２は、暗号化されたワークキーＫｗを受理して、Ｋｗ解読手段２０３に送る手段である。更に又、受信側認証手段２０２は、ＳＴＢ１００から送られてくる関数識別子ｉをＫｃ生成関数選択手段２０４に、又、乱数Ｋｃ′[ｎ]をＫｃ生成手段２０５に出力する手段である。

【００５３】暗号解読手段２０６は、ＳＴＢ１００から転送されてきた暗号化されたＡＶデータをワークキーＫｗを用いて解読し、記録・再生手段（図示省略）１０３４へ出力する手段である。Ｋｃ生成関数選択手段２０４は、ＳＴＢ１００が内蔵している上記複数個の関数と同じ関数を、予め内蔵しており、入力されてきた関数識別子ｉに対応する関数ｆｉを抽出して、Ｋｃ生成手段２０５へ出力する手段である。この関数ｆｉは、数１で表せる。Ｋｃ生成手段２０５は、Ｋｃ履歴記憶手段２０７か

ら読み出した１つ前と２つ前に使用していたコントロールキーＫｃと、受信側認証手段２０２から出力された乱数Ｋｃ′とを、関数ｆｉの変数として利用して、新たなコントロールキーＫｃを生成する手段である。この新たなＫｃは、数２で表せる。又、Ｋｃ履歴記憶手段２０７は、Ｋｃ生成手段２０５により生成されたコントロールキーＫｃの履歴を記憶しておく手段である。尚、ＳＴＢ１００と他の端末装置との間で、既にデータの転送が行われている最中に、ＶＴＲ装置２００が途中からデータの転送を受ける場合には、Ｋｃ履歴記憶手段２０７は、次のような例外的な動作を行う手段である。即ち、その場合、Ｋｃ履歴記憶手段２０７は、上記他の端末装置との間で現に使用しているコントロールキーと、その１つ前に使用していたコントロールキーとをＳＴＢ１００から受け取り、それらを記憶する手段である。

【００５４】尚、受信側認証手段２０２は、図６で述べた、認証手段１０３２と同様に、秘密関数Ｓａを有している。

【００５５】以上の構成において、次に、図１、図２を参照しながら、本実施の形態の動作を説明する。

【００５６】ここでは、まず、（１）ＳＴＢ１００が、ＶＴＲ装置２００のみに対してＡＶデータの転送を開始する場合を述べ、その後、（２）上記（１）の動作中に、別の受信端末装置すなわち、記録装置４００に対するデータ転送が開始される場合を中心に説明する。

【００５７】（１）上述した通り、ここでは、ＳＴＢ１００からＶＴＲ装置２００へのみ、ＡＶデータを転送する場合について述べる。

【００５８】ＶＴＲ装置２００が、所望のＡＶデータをＳＴＢ１００から転送してもらうためには、ＳＴＢ１００とＶＴＲ装置２００との間で、図６で述べたのと同様の認証・鍵交換の動作を行った後、本実施の形態の特有の動作を行うものである。

【００５９】ステップ１０１：即ち、ここでは、認証要求手段２０１により、ＳＴＢ１００に対して認証・鍵交換の動作の開始の要求が行われる。その後の認証・鍵交換の動作の詳細は、以下の点を除き、上述したステップ１００１～１００７で述べたものと同様であるので、その説明は省略する。尚、この認証・鍵交換の動作においては、ＶＴＲ装置２００における乱数Ａ１，Ａ２の発生は、受信側認証手段２０２が行い、ＳＴＢ１００における乱数Ｂ１，Ｂ２の発生は、乱数発生手段１０４が行う。又、上記ステップ１００１～１００７の動作において、認証が成立した場合、図６で述べた通り、双方の装置においてサブキーＫｓａが生成される。その後の、認証・鍵交換の動作において最初にＶＴＲ装置２００へ転送されるキーは、本実施の形態では、ステップ１０２で述べるように２個であり、この点は従来と異なる。

【００６０】ステップ１０２：即ち、乱数発生手段１０４で発生された２つの乱数をダミーキーＫｃ[0]と、コントロールキーＫｃ[1]と定義する。このダミーキーＫｃ[0]と、コントロールキーＫｃ[1]は、送信側認証手段１０２へ送られる。又、コントロールキーＫｃ[1]は、Ｋｗ暗号化手段１０７にも送られる。

【００６１】即ちこの場合、Ｋｃ[0]、及びＫｃ[1]の生成については、数２を使用せず、例外的処置として、乱数発生手段１０４により発生される乱数を使用するものとする。

【００６２】ステップ１０３：さらに、これら２つのキーＫｃ[0]及びＫｃ[1]は、Ｋｃ記憶手段１０５に記憶される。又、Ｋｃ生成関数選択手段１０３により選択された関数ｆｉが、Ｋｃ生成手段１０６に送られ、それに対応する関数識別子ｉが送信側認証手段１０２に送られる。尚、関数ｆｉは、必要に応じて、更新しても良い。

【００６３】ステップ１０４：送信側認証手段１０２では、上記のようにして送られてきたダミーキーＫｃ[0]とコントロールキーＫｃ[1]が、サブキーＫｓａにより暗号化されて、Ｋｓａ（Ｋｃ[0]，Ｋｃ[1]）として、データ転送手段１０２４へ送られる。さらに、Ｋｓａ（Ｋｃ[0]，Ｋｃ[1]）は、データ転送手段１０２４から、ＶＴＲ装置２００へ転送される。図２では、この転送に、符号６０１を付した。ここで、図２は、コントロールキーの更新に伴い行われる、ＳＴＢ１００から受信端末装置２００、４００への転送の状況を中心に示した模式図である。同図において、縦軸は時間であり、図中の上から下へ向けて時間が経過している。

【００６４】尚、この転送６０１の際、Ｋｃ生成関数ｆｉに対応する関数識別子ｉも、ＶＴＲ装置２００に転送される。

【００６５】ステップ１０５：ＳＴＢ１００から転送されてきたＫｓａ（Ｋｃ[0]，Ｋｃ[1]）と関数識別子ｉは、データ転送手段１０３１により、受信側認証手段２０２へ送られる。

【００６６】ステップ１０６：そして、受信側認証手段２０２は、Ｋｓａ（Ｋｃ[0]，Ｋｃ[1]）を解読し、前後に配置された２つのキーの内、予め定められている通り、後ろに配置されたＫｃ[1]を抽出し、Ｋｗ解読手段２０３へ送る。又、受信側認証手段２０２は、関数識別子ｉをＫｃ生成関数選択手段２０４へ送る。そして、Ｋｃ生成関数選択手段２０４が、その識別子ｉに対応する関数ｆｉを抽出して、Ｋｃ生成手段２０５へ送る。尚、解読されたＫｃ[0]，Ｋｃ[1]は、共に、Ｋｃ生成手段２０５を介して、Ｋｃ履歴記憶手段２０７に送られ、記憶される。

【００６７】ステップ１０７：一方、Ｋｗ暗号化手段１０７がコントロールキーＫｃ[1]を用いて暗号化したワークキー、即ち、Ｋｃ[1]（Ｋｗ）は、送信側認証手段１０２及びデータ転送手段１０２４を経て、ＶＴＲ装置２００に転送される。

【００６８】ステップ１０８：ＶＴＲ装置２００に送ら

れてきたＫｃ[1]（Ｋｗ）は、受信側認証手段２０２を経て、Ｋｗ解読手段２０３に送られる。Ｋｗ解読手段２０３は、ステップ１０６において送られてきたコントロールキーＫｃ[1]を用いて、Ｋｃ[1]（Ｋｗ）を解読して、Ｋｗを暗号解読手段２０６に送る。

【００６９】ステップ１０９：一方、ＳＴＢ１００の暗号化手段１０１により暗号化されたＡＶデータであるＫｗ（ＡＶ）の転送が、データ転送手段１０２４を介して開始される。

【００７０】ステップ１１０：Ｋｗ（ＡＶ）は、データ転送手段１０３１から暗号解読手段２０６へ送られる。暗号解読手段２０６は、Ｋｗ解読手段２０３から送られてきたＫｗを用いて、Ｋｗ（ＡＶ）を解読し、記録・再生手段に出力する。

【００７１】次に、ステップ１１０において、解読されたＡＶデータが記録・再生手段に出力されている途中で、コントロールキーＫｃが更新される場合の動作を述べる。

【００７２】ステップ２０１：本実施の形態では、コントロールキーを定期的に更新するものとし、乱数発生手段１０４が、乱数Ｋｃ′を定期的に発生させる。即ち、１回目の更新に利用する乱数Ｋｃ′[1]が、乱数発生手段１０４からＫｃ生成手段１０６と、送信側認証手段１０２に送られる。

【００７３】ステップ２０２：送信側認証手段１０２に送られた乱数Ｋｃ′[1]は、データ転送手段１０２４を介して、ＶＴＲ装置２００へ転送される。図２では、この転送に符号６０２を付した。

【００７４】ステップ２０３：Ｋｃ生成手段１０６は、Ｋｃ記憶手段１０５に記憶されているＫｃ[0]及びＫｃ[1]を読み出して、乱数発生手段１０４から送られてきた乱数Ｋｃ′[1]と共に、関数ｆｉ（数２参照）の変数として用いる。

【００７５】この場合、生成される新たなコントロールキーＫｃ[2]は、数２より、Ｋｃ[2]＝ｆｉ（Ｋｃ′[1]，Ｋｃ[0]，Ｋｃ[1]）と表せる。尚、Ｋｃ[2]は、Ｋｃ記憶手段１０５に記憶される。

【００７６】ステップ２０４：新たなコントロールキーＫｃ[2]は、Ｋｗ暗号化手段１０７へ送られ、ワークキーＫｗの暗号化に用いられる。暗号化されたワークキーであるＫｃ[2]（Ｋｗ）は、ステップ１０７と同様にしてＶＴＲ装置２００へ転送される。

【００７７】ステップ２０５：又、ステップ２０２において、ＶＴＲ装置２００に転送された乱数Ｋｃ′[1]は、データ転送手段１０３１から受信側認証手段２０２に送られ、さらにＫｃ生成手段２０５に送られる。

【００７８】ステップ２０６：Ｋｃ生成手段２０５では、Ｋｃ履歴記憶手段２０７に記憶されているＫｃ[0]及びＫｃ[1]と読み出して、ステップ２０５において送られてきた乱数Ｋｃ′[1]と共に、関数ｆｉ（数２参照）の変数として用いる。この場合、生成される新たなコントロールキーＫｃ[2]は、ステップ２０３で述べたものと同じであり、Ｋｃ[2]＝ｆｉ（Ｋｃ′[1]，Ｋｃ[0]，Ｋｃ[1]）と表せる。尚、Ｋｃ[2]は、Ｋｃ履歴記憶手段２０７に記憶される。

【００７９】ステップ２０７：新たなコントロールキーＫｃ[2]は、Ｋｗ解読手段２０３へ送られ、Ｋｃ[2]で暗号化されたワークキーＫｗの解読に用いられる。解読されたワークキーＫｗは暗号化解読手段２０６に送られる。

【００８０】ステップ２０８：ステップ１１０と同様の動作が行われる。

【００８１】次に、ステップ２０８において、解読されたＡＶデータが記録・再生手段に出力されている途中で、コントロールキーＫｃ[2]が、さらに更新される場合の動作を述べる。ここでは、すでに述べた内容と同様の点が多いので、数２に関する特徴点のみについて述べる。

【００８２】即ち、ここで生成されるコントロールキーＫｃ[3]は、数２のｎに２を代入することにより次のように表せる。図２では、乱数Ｋｃ′[2]の転送に符号６０３を付した。

【００８３】

【数３】

Ｋｃ[3]＝ｆｉ（Ｋｃ′[2]，Ｋｃ[1]，Ｋｃ[2]）

上記（数３）及び（数２）から明らかなように、本実施の形態においては、２回目の更新以降に生成されるコントロールキーは、１つ前、及び２つ前に使用したコントロールキーと、乱数発生手段１０４により更新の度に発生される乱数Ｋｃ′と、それらを変数とする関数ｆｉとにより生成されるものである。

【００８４】以上述べた様に、本実施の形態によれば、認証動作を繰り返すことなく、過去に使用したコントロールキーの履歴と乱数とを用いてコントロールキーを更新することにより、コントロールキーの信頼性をより一層向上させることが出来る。

【００８５】（２）上記（１）の動作において、コントロールキーの２回目の更新が行われた後に、記録装置４００に対するデータ転送が開始される場合について、図２を参照しながら述べる。

【００８６】ステップ３０１：ＳＴＢ１００と、新たに転送要求を行う記録装置４００との間において、ステップ１０１と同様の認証動作が行われる。

【００８７】ステップ３０２：認証が成立した後、送信側認証手段１０２は、Ｋｃ記憶手段１０５に記録されている、現在使用中のコントロールキーＫｃ[3]とその１つ前に使用していたコントロールキーＫｃ[2]とを読み出して、サブキーＫｓｃにより暗号化する。そして、このＫｓｃ（Ｋｃ[2]、Ｋｃ[3]）と、現在使用中の関数ｆｉに対応する関数識別子ｉとをデータ転送手段１０２

４を介して、記録装置４００へ転送する（図２では、この転送に符号６０４を付した）。尚、サブキーＫｓｃは、上記認証動作により上記と同様の方法により生成されたものである。

【００８８】ステップ３０３：記録装置４００では、受信側認証手段２０２が、上記のようにして送られてきたＫｓｃ（Ｋｃ[2]、Ｋｃ[3]）を、サブキーＫｓｃを用いて解読し、Ｋｃ[3]を抽出する。この解読・抽出の動作と、その後のＫｃ生成関数選択手段２０４及びＫｃ履歴記憶手段２０７などの動作は、ステップ１０６で述べた内容と同じである。

【００８９】ステップ３０４：一方、ＳＴＢ１００では、Ｋｗ暗号化手段１０７が、現在使用中のコントロールキーＫｃ[3]を用いて、ワークキーＫｗを暗号化したＫｃ[3]（Ｋｗ）を記録装置４００に転送する。このＫｃ[3]（Ｋｗ）は、ＶＴＲ装置２００に転送したものと同じである。

【００９０】ステップ３０５：記録装置４００での、Ｋｃ[3]（Ｋｗ）の解読動作は、ステップ１０８の内容と同じである。

ステップ３０６：暗号化されたＡＶデータの転送動作は、ステップ１０９の内容と同じである。

【００９１】ステップ３０７：記録装置４００での、ＡＶデータの解読動作は、ステップ１１０の内容と同じである。

【００９２】次に、コントロールキーＫｃ[3]が更新される場合の動作は、上記ステップ２０１～２０８での説明において、Ｋｃ[0]をＫｃ[2]と読み替え、Ｋｃ[1]をＫｃ[3]と読み替え、かつ、乱数Ｋｃ′[1]を乱数Ｋｃ′[3]と読み替えたものと同じである。

【００９３】ここで生成されるコントロールキーＫｃ[4]は、数２のｎに３を代入することにより次のように表せる。図２では、乱数Ｋｃ′[3]の転送に符号６０５を付した。

【００９４】

【数４】

Ｋｃ[4]＝ｆｉ（Ｋｃ′[3]，Ｋｃ[2]，Ｋｃ[3]）

この様に、途中からＡＶデータの転送を受ける端末装置が現れて、受信端末が増加しても、ＳＴＢ１００が使用するコントロールキーは、受信端末装置の数に関係なく共通したものとなる。

【００９５】これにより、不正者が、たまたま、これまで使用されてきたコントロールキーの内、いずれか一つを、例えば、総当たり計算等により解いたとしても、それまでのコントロールキーの履歴と、それとは別の乱数との組み合わせにより、コントロールキーが生成されるため、不正解読されたコントロールキー以降に生成されたコントロールキーが連鎖的に解かれてしまうことを防止出来る。

【００９６】又、コントロールキーの更新に使用する乱数Ｋｃ′が、不正者により傍受されたとしても、それ以前のコントロールキーの履歴が分からなければ、コントロールキーの解読は不可能である。

【００９７】尚、上記実施の形態では、先に発生させた乱数と、過去のコントロールキーＫｃとを利用して、関数ｆｉ（第１の関数）により新たなコントロールキーＫｃを生成する場合について述べたが、これに限らず例えば、次の様な構成のデータ送信装置としても良い。即ち、具体的には、図３に示す様に、上記Ｋｃ生成手段１０６に代えて、（１）新たなコントロールキーＫｃを生成するコントロールキー生成手段１１０６と、上記乱数発生手段１０４に代えて、（２）過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数Ｆｉとを利用して、秘密要素Ｋｃ′を生成する秘密要素生成手段１１０４とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素Ｋｃ′を、前記第２の関数の逆関数$F^{-1}i$を有するデータ受信装置１２００に転送する構成のデータ送信装置１１００であっても良い。一方、データ受信装置１２００には、図３に示すように、第２関数選択手段１１０３が有する複数個の第２関数に対応する逆関数を備えた逆関数選択手段１２０４が設けられている。この逆関数選択手段１２０４は、受信側認証手段２０２からの関数識別子ｉを得て、それに対応する逆関数$F^{-1}i$を選択し、Ｋｃ生成手段２０５へ送る。Ｋｃ生成手段２０５は、送られてきた逆関数$F^{-1}i$を用いて、受信側認証手段２０２からの秘密要素Ｋｃ′と過去のコントロールキーＫｃを変数として、上記と同様に新たなコントロールキーＫｃを生成する。

【００９８】又、上記実施の形態では、認証が成立した場合、初回の転送６０１（図２参照）で、ワークキーＫｗの暗号化に最初に使用するコントロールキーＫｃ[1]と、そのコントロールキーの更新に利用するキーＫｃ[0]とを暗号化して転送する場合について述べたが、これに限らず例えば、データ受信装置が有する第１の関数（例えば、関数ｆｉ）または上記逆関数$F^{-1}i$の変数がコントロールキーＫｃを生成するのに不足している時期においては、前記コントロールキーＫｃを含む暗号情報を初期情報として、前記データ受信装置に転送する構成のデータ送信装置であっても良い。即ち、具体的には、例えば、図４に示すように、ＳＴＢ２１００は、転送１６０２において、Ｋｓａ（Ｋｃ[1]，Ｋｃ[2]）を転送する。転送１６０２では、すでに行った認証・鍵交換により生成されたサブキーＫｓａをそのまま使用するので、新たなサブキーの生成作業は不要である。データ受信装置としてのＶＴＲ装置２２００は、転送されてきたＫｓａ（Ｋｃ[1]，Ｋｃ[2]）を解読し、Ｋｃ[2]を抽出する。

【００９９】又、これとは別の例として、データ受信装

置が有する第１の関数ｆｉ又は上記逆関数F^{-1}ｉの変数が、コントロールキーＫｃを生成するのに不足している時期においては、秘密要素（例えば、乱数Ｋｃ′）を含む前記不足している変数を初期情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図５に示すように、例えば、上記実施の形態の（数２）を利用した場合について述べると、次の式（数５）により表せるコントロールキーＫｃが、双方の装置において、関数ｆｉを利用して生成されるものである。

【０１００】

【数５】

Ｋｃ[１]＝ｆｉ（Ｋｃ′[０]，Ｋｃ[－１]，Ｋｃ[０]）

ここで、Ｋｃ′[０]は、データ送信装置で発生された乱数等の秘密要素であり、Ｋｃ[－１]、Ｋｃ[０]は、それまでに未使用のコントロールキーである。これら未使用のコントロールキーは、乱数として発生させても良いし、予め、内蔵されている複数個の中から抽出しても良い。この場合、図５に示す転送２６０１において、データ送信装置としてのＳＴＢ３１００からデータ受信装置としてのＶＴＲ装置３２００に対して、コントロールキーＫｃ[１]の生成に必要な変数として、Ｋｃ′[０]とＫｃ[－１]とＫｃ[０]とをサブキーにより暗号化して転送する必要がある。

【０１０１】又、これとは別の例として、データ受信装置が有する第１の関数又は上記逆関数の変数が、コントロールキーＫｃを生成するのに不足している時期の内、（１）前半においては、前記コントロールキーＫｃを含む暗号情報を初期前半情報として、又、（２）後半においては、前記秘密要素を含む前記不足している変数を初期後半情報として前記データ受信装置に転送する構成のデータ送信装置であってもよい。即ち、具体的には、図２の転送６０１に代えて、Ｋｓａ（Ｋｃ[1]）を転送し、同図の転送６０２に代えて、秘密要素としてのＫｃ′[１]と、上記不足している変数としてのＫｃ[０]とを転送するものである。これにより、転送６０１の結果、データ受信装置においてＫｃ[１]が抽出され、最初のコントロールキーとして使用される。又、データ受信装置では、この様にして抽出されたコントロールキーＫｃ[１]と、転送６０２により入手したＫｃ′[１]及びＫｃ[０]とを変数として、関数ｆｉにより次のコントロールキーＫｃ[２]を生成する。

【０１０２】又、上記実施の形態では、Ｋｃ生成関数を予め複数個有しており、その中から一つを選択して使用する場合について述べたが、これに限らず例えば、認証動作の際に、使用する関数そのものを転送する構成でも良いし、あるいは、関数は、はじめから固定されていても良い。

【０１０３】又、上記実施の形態では、先に発生させた乱数と、過去のコントロールキーＫｃとを利用して、関数ｆｉ（第１の関数）により新たなコントロールキーＫｃを生成する場合について述べたが、これに限らず例えば、新たなコントロールキーＫｃを生成するコントロールキー生成手段と、過去に生成されたコントロールキーＫｃの全部又は一部と前記新たに生成されたコントロールキーＫｃと、それらを変数とする第２の関数とを利用して、秘密要素を生成する秘密要素生成手段とを備え、前記コントロールキーＫｃが新たに更新される場合、前記秘密要素を、前記第２の関数の逆関数を有するデータ受信装置に転送する構成のデータ送信装置であっても良い。

【０１０４】又、上記実施の形態では、新たなコントロールキーＫｃを生成する際、コントロールキーＫｃの履歴として、１つ前と２つ前のものを変数として用いる場合について述べたが、これに限らず例えば、過去に使用したコントロールキーであれば、２つ前と３つ前、若しくは、１つ前と３つ前等どれでも良い。又、過去のコントロールキーＫｃであれば、その個数は、２個に限らず、例えば、１個以上であれば、幾つでも良く、記憶容量が確保出来るならば、過去に使用した全てのコントロールキーを用いてもかまわない。

【０１０５】又、以上述べた実施の形態の何れか一つに記載の各手段またはステップの全部又は一部の手段またはステップをコンピューターに実行させるためのプログラムを記録した磁気記録媒体や光記録媒体などを作成し、これを利用して上記と同様の動作を実行させることも出来る。この場合も上記と同様の効果を発揮する。

【０１０６】又、上記実施の形態の各手段又はステップの処理動作は、コンピュータを用いてプログラムの働きにより、ソフトウェア的に実現してもよいし、あるいは、上記処理動作をコンピュータを使用せずに特有の回路構成により、ハード的に実現してもよい。

【０１０７】

【発明の効果】以上述べたところから明らかなように本発明は、従来に比べて実質上の負担を増やすことなくコントロールキーの秘密保持についての信頼性を従来に比べてより一層向上させることが出来るという長所を有する。

【図面の簡単な説明】

【図１】本発明の一実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図２】同実施の形態において、コントロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図３】本発明の他の実施の形態におけるデータ送信装置及びデータ受信装置の構成を示す構成図

【図４】本発明の別の実施の形態において、コントロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図５】本発明のさらに別の実施の形態において、コン

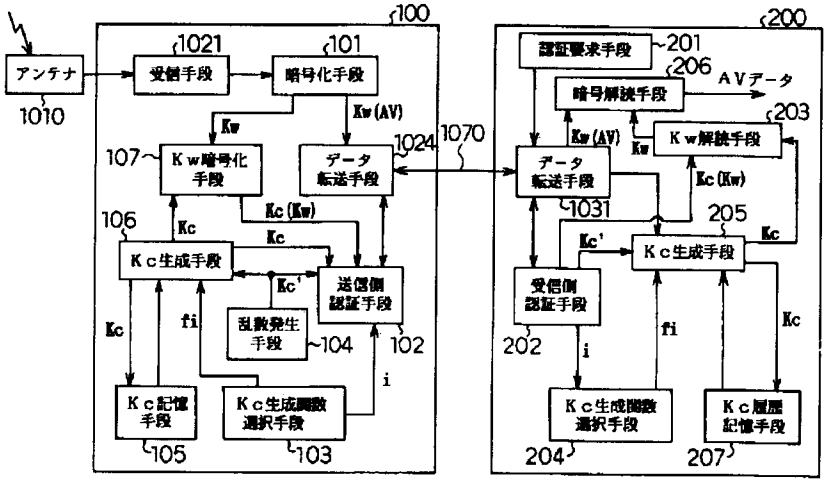
トロールキーの更新に伴い行われる、ＳＴＢから受信端末装置への転送の状況を中心に示した模式図

【図６】従来のデータ送信装置及びデータ受信装置の構成を示す構成図

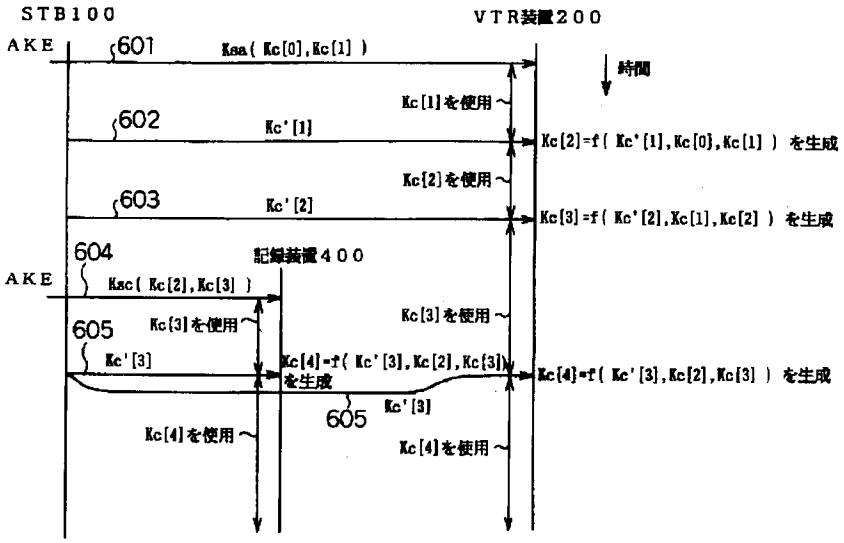
【符号の説明】

１００　ＳＴＢ
１０１　暗号化手段
１０２　送信側認証手段
１０３　Ｋｃ生成関数選択手段
１０４　乱数発生手段
１０５　Ｋｃ記憶手段
１０６　Ｋｃ生成手段
１０７　Ｋｗ暗号化手段

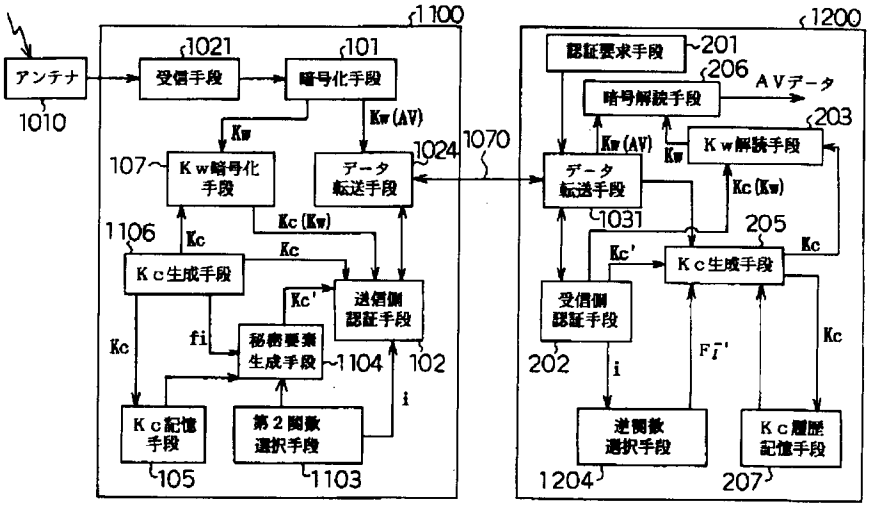
【図１】



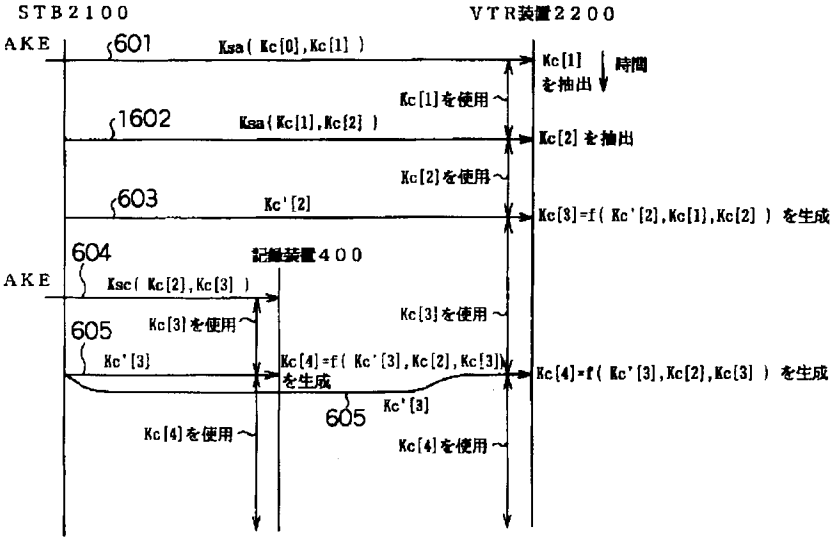
【図２】



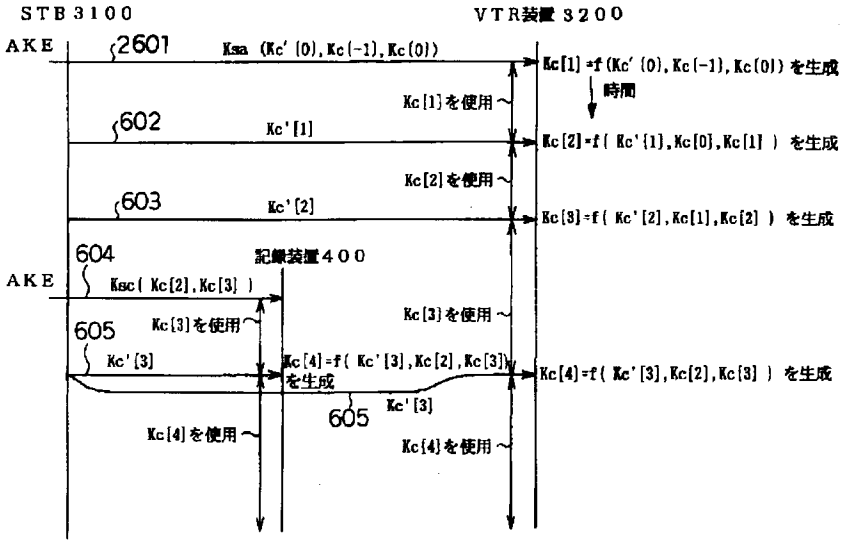
【図３】


1100
1200
アンテナ
1010
1021
受信手段
101
暗号化手段
Kw(AV)
Kw
107
Kw暗号化手段
1024
データ転送手段
1070
1106
Kc
Kc生成手段
Kc(Kw)
Kc'
送信側認証手段
102
fi
秘密要素生成手段
1104
i
Kc記憶手段
105
第２関数選択手段
1103
認証要求手段
201
206
AVデータ
暗号解読手段
203
Kw解読手段
データ転送手段
1031
205
Kc生成手段
受信側認証手段
202
逆関数選択手段
1204
Kc履歴記憶手段
207

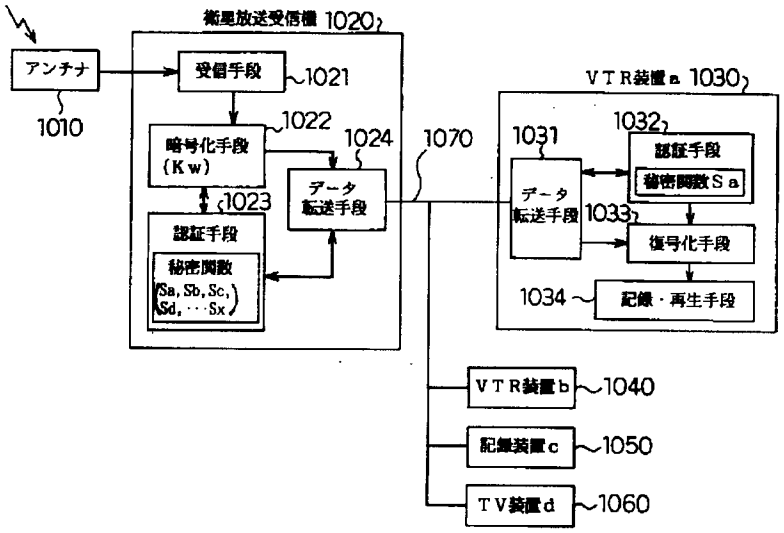
【図４】


STB2100
VTR装置2200
AKE
601
Ksa(Kc[0],Kc[1])
Kc[1]を抽出
時間
Kc[1]を使用
1602
Ksa(Kc[1],Kc[2])
Kc[2]を抽出
Kc[2]を使用
603
Kc'[2]
Kc[3]=f(Kc'[2],Kc[1],Kc[2]) を生成
604
記録装置400
AKE
Ksc(Kc[2],Kc[3])
Kc[3]を使用
Kc[3]を使用
605
Kc'[3]
Kc[4]=f(Kc'[3],Kc[2],Kc[3])を生成
Kc[4]=f(Kc'[3],Kc[2],Kc[3]) を生成
605
Kc'[3]
Kc[4]を使用
Kc[4]を使用

【図５】



【図６】



フロントページの続き

(72)発明者　後藤　昌一
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　武知　秀明
大阪府門真市大字門真1006番地　松下電器産業株式会社内